UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,255	12/28/2000	Theodore Jack London Shrader	AUS920000851US1	7414

7590 03/08/2006

Darcell Walker
8107 Carvel Lane
Houston, TX 77036

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/750,255
Filing Date: December 28, 2000
Appellant(s): SHRADER ET AL.

Darcell Walker
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/21/05 appealing from the Office action mailed 4/21/05.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence relied upon

- **Sudia, US patent 6,209,091**
- "How the Internet Works", 4th edition, 1998, page 19, Item 4.
- Internet Explorer 3 for Windows for Dummies, Doug Lowe, IDG Books, 1996, pages 139-153.

- audit trail

  A record of business transactions that can be used by an interested party to trace an organization's activities to original documents. Audit trails are used to verify account balances.

- Source: *Wall Street Words: An A to Z Guide to Investment Terms for Today's Investor by David L. Scott.*
  Copyright © 2003 by Houghton Mifflin Company. Published by Houghton Mifflin Company.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

5. Claims 1-18 rejected under 35 U.S.C. 102(e) as being anticipated by Sudia et al.

6. Claims 1, 10 are additionally rejected under 35 U.S.C. 102(b) as being anticipated by Internet Explorer 3 for Windows for Dummies, Doug Lowe, IDG Books, 1996, pages 139-153.

In reference to claim 1 and 10:

"Internet Explorer 3 for Windows for Dummies" discloses a general communication transmission method that enables a transmitted message to span synchronous and asynchronous protocols over a computer network during one transmission comprising:

- Packaging a message for transmission in a data object, the message packages including information on the original message in the transmission and email attachments, and the data object is an email. ("sending electronic email" p. 141)
- Sending the packaged message to a designated recipient entity, where the message is transmitted to the recipient of the email. ("sending electronic email" p. 141)
- Receiving the message by a current recipient entity at a location, where the email may be received by the recipient at a personal computer. ("receiving electronic email" p. 151-152)
- Recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message, where the event is recorded in the user's Email client which shows that emails were received. (Figure 11-1, page 140)
- Determining whether the current recipient entity is the designated recipient entity, where the email server which is inherent to email systems, determine whether the current recipient entity is the designated entity and then proceed to send email to that entity. (ex. An email for asdf@asdf.com will not goto qwer@qwer.com)

In reference to claims 1 and 10:

Sudia et al. (Column 16, line 20 – Column 18, line 20) discloses a general communication transmission method that enables a transmitted message to span synchronous and asynchronous protocols over a computer network during one transmission comprising:

- packaging a message for transmission in a data object, where the message is the document, and the data object it is packed in also contains the header. (Column 16, lines 30-37) the message packages further including information on the original message in the transmission; (Column 16, lines 30-37)
- sending the packaged message to a designated recipient entity, where the recipient entities include the authorizing agents and the signing devices. (Column 16, lines 54- Column 17, lines 11)
- receiving the message by a current recipient entity at a location, where the locations include the authorizing agents and the signing devices. (Column 16, lines 54- Column 17, lines 11)
- Recording the event of receiving the packaged message information by current recipient in a message transmission history generated for the transmitted message, where the message transmission history is indicated by each of the parties that signed the document as it passes through the network. (Column 16, lines 45-52) & (Column 16, lines 57-65) & Figure 10.
- determining whether current recipient entity is the designated recipient entity, where the designated recipient entity is checked by examining whether at each

point, the entity has received the quorum of digital signatures. (Column 17, lines 13-18) & (Column 17, lines 38-45)

In reference to claim 2:

Sudia et al. (Column 16, line 65 – Column 17, line 5) & (Column 17, lines 13-18) discloses a method as described in claim 1 comprising before said designated recipient determining step, the step of modifying the packaged message information in indicate that the current recipient entity received the package message by adding substantive information to said packaged message, where the substantive information to each packaged message includes a new header, and or partial digital signature, and indicates the recipient received the message.

In reference to claim 3:

Sudia et al. (Column 16, line 20 – Column 18, line 20) discloses the method as described in claim 1 wherein said message package is a data object with data fields containing the original message, signing certificate. signature bytes and signed attributes and wherein modification of the message package comprising creating a new data object that is added to the original data object, the new data object having additional information concerning the transmission, where the message package is further modified by affixing an additional signature which is added to the original data object, where the data object contained the original message, signing certificate, signature bytes, and other signed attributes, and

where the new data object afterwards has information concerning the transmission. (Column 16, lines 54-65)

In reference to claim 4:

Sudia et al. (Column 9, lines 50-52) & (Column 10, lines 25-35) discloses a method as described in claim 1 wherein each recipient entity uses a public key and private key pair to authenticate the packaged message origin and contents.

In reference to claim 5:

Sudia et al. (Column 10, lines 10-22) discloses a method as described in claim 4 further comprising verifying the packaged message by a recipient entity using the sending entities public key, where the public key is the public signature verification key.

In reference to claim 6:

Sudia et al. (Column 16, lines 54-65) discloses a method as described in claim 1 wherein said step of determining whether current recipient entity is the designated recipient entity comprises determining whether the packaged message received by said recipient entity has an existing message, where the packaged message is unpackaged to determine whether the designated entity should be the one to sign the document.

In reference to claim 7:

Sudia et al. (Column 16, line 20 – Column 18, line 20) discloses a system for transmitting messages spanning synchronous and asynchronous protocols over a compute: network comprising:

- a network transmission mechanism that enables transmissions across synchronous and asynchronous protocols, where the network transmission mechanism that allows transmissions across synchronous and asynchronous protocols is the sealed message/object and the audit trail (Column 16, lines 54-65)
- a data structure for containing the information message transmitted over the computer network the data structure having multiple fields for containing various items related to the message being transmitted; and encryption key pairs to ensure authenticity and integrity of the message during transmission between sender and final receiver sites, where public and private key cryptography are used and the data structure has multiple fields for containing various items related to the message such as the digital signatures. (Column 16, lines 44-53) & (Column 9, lines 45-55)
- a message transmission history file containing events of each of a stop a transmitted message in route to the message destination, where the message transmission history file is the document being sent, which is modified by each destination en route with the final message destination, thereby containing events of each stop. (Figure 10)

In reference to claim 8:

Sudia et al. (Column 16, lines 30-65) discloses a system as described in claim 7 wherein said data structure contains information comprising original message, signing certificate, signature bytes and signed attributes, where the original message is the document of transmission, where the signing certificate is the signed certificate (Column 16, lines 49-51), where the signature bytes are the bytes of the actual signature, and the signed attributes includes the hash, the audit trail, and the multiple signatures, as well as other attributes indicative of a signature.

In reference to claim 9:

Sudia et al. (Column 16, lines 30-65) discloses a system as described in claim 7 further comprising additional data structures that can be linked and thereby added to the data structure of the original message at each receipt of the message during transmission, said additional data structures containing information about the message transmission, where the additional data structures are the additional signatures and partial signatures affixed which contain information about the message transmission (the audit trail)

Claims 10-18 are rejected for the same reasons as claims 1-9 respectively.

In support of the inherency with respect to the rejection of claim 1 under "Internet Explorer 3 for Windows for Dummies", the Examiner provides the following support:

- "Internet Explorer 3 for Windows for Dummies", page 143
- "How the Internet Works", 4th edition, 1998, page 19, Item 4.

(10) Response to Arguments

10a) (response to arguments presented in section 6a)

The Appellant argues that Sudia does not recite the step of recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message.

With regards to the recording of the event in a message transmission history, the Examiner has cited Sudia, (Column 16, lines 45-52) & (Column 16, lines 57-65) & Figure 10. as well as the greater recitation of Sudia (Column 16, line 20 – Column 18, line 20) in order to provide for additional background information to properly interpret the substance of (Column 16, lines 45-52) & (Column 16, lines 57-65) & Figure 10 as cited in the rejection.

Sudia discloses a system in which a message or document will be transmitted through a series of nodes. As the message transmission passes through each node, each node will affix a digital signature to the message as an audit trail so it can be determined which nodes it has passed through.

1) Sudia (Column 16, lines 20-26) gives background information and states that Figures 9 and 10 illustrate the flow of the document through various authorizing agents and signing devices, while figure 10 illustrates the evolution of signatures on the document.

2) When satisfied that the document should be signed, Authorizing agent 1a (AA1a) signs the document using the Agent's secret signature key. The signed transmission is then sent to Authorizing agent 1b. (Column 16, lines 45-53)

3) Authorizing agent 1b, after performing its checks, also signs the document. Sudia (Column 16, lines 63-65) explicitly states AA1a's signature is left on the document as an audit trail. AA1b then affixes a new header and sends the twice signed document to Signing Device 1.

Sudia (Column 17, lines 50-57) additionally discloses that "in the example described above, two signing devices were necessary to affix the system wide authority signature... The total number of signing devices needed to complete a signature in a system may be adjusted at the time the key shares are generated"

The Examiner contends that because Sudia explicitly stated that the signatures as the document passes through the nodes are left "as an audit trail" (Column 16, line 63), the series of signatures may be considered a "transmission history". An audit trail is commonly understood as such: (taken from www.dictionary.com)

audit trail

A record of business transactions that can be used by an interested party to trace an organization's activities to original documents. Audit trails are used to verify account balances.

Source: *Wall Street Words: An A to Z Guide to Investment Terms for Today's Investor by David L. Scott.*

10b) Response to arguments presented in section 6b.

The Appellant argues that "Keeping in Touch with Microsoft Internet Mail" does not disclose "the step of recording the event of receiving the packaged message by a current recipient in a message transmission history."

The Examiner's citation to that particular claimed element is (Figure 11-1, page 140)

Figure 11-1 discloses a column in the Internet mail entitled "Received"

Figure 11-1 discloses emails received from "Dwight Miyake" on 6/25/96, 7:01 PM with the subject "nice page Douglas!" , and "Colleen Rainsberger" on 6/25/96 2:23 PM, 12:28 PM and 12:28 PM with the respect subjects "Re: Status", "page count", "Re: Status".

With each message or transmission, it can be determined who a message was sent from, along with the date and time of transmission and reception, along with a subject header to broadly summarize the subject matter of the message.

The Examiner contends that one of ordinary skill in the art would interpret this history as a "step of recording the event of receiving the packaged message by a current recipient in a message transmission history generated for the transmitted message".

For these reasons, the Examiner has maintained his rejections of the claims with respect to the arguments presented by the Applicant.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thomas M Ho

Examiner 2134

Conferees:

Gilberto Barron

SPE 2132

Kambiz Zand

Primary 2132

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

How the Internet Works

Fourth Edition

Preston Gralla

Illustrated by Sarah Ishida, Mina Reimer, and Stephen Adams

A division of Macmillan Computer Publishing, USA
201 W. 103rd Street
Indianapolis, IN 46290

First printing: September 1998

Executive Editor	Karen Reinisch
Acquisitions Editor	Renee Wilmeth
Development Editor	Noelle Gasco
Technical Editor	Doug Klippert
Managing Editor	Thomas F. Hayes
Project Editor	Karen A. Walsh
Copy Editors	Barbara Hacha and Julie McNamee
Illustrators	Sarah Ishida, Mina Reimer, and Stephen Adams
Book Designers	Carrie English and Bruce Lundquist
Production	Betsy Deeter, Lisa England, John Etchison, and Trina Wurst
Indexers	Sandra Henselmeier and Cheryl Jackson

Library of Congress Catalog No.: 98-85292

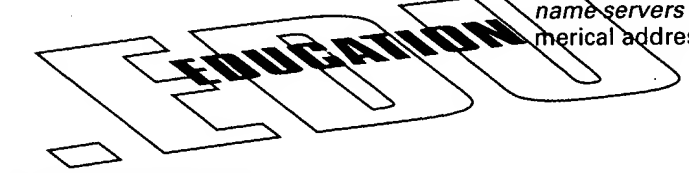
ISBN: 0-7897-1726-3

00 99 6 5 4 3

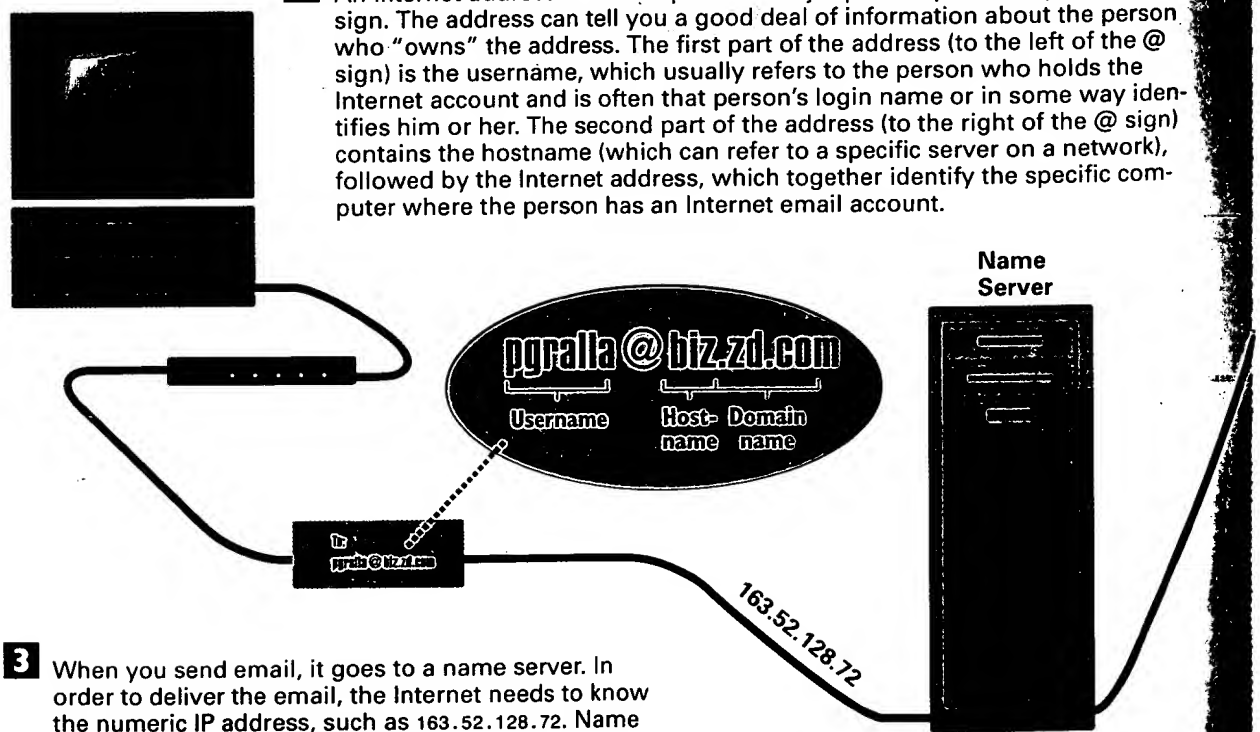
Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit number, the number of the book's printing. For example, a printing code of 98-1 shows that the first printing of the book occurred in 1998.

How Internet Addresses and Domains Work

1 The Internet Protocol (IP) delivers mail based on the specific email address. This address is expressed as four numbers, separated by periods (called dots), such as 163.52.128.72. However, because it would be difficult to remember such complex addresses, you can instead use Internet addresses made up of words and letters. Computers called *domain name servers* translate the alphabetical address into a numerical address, so email can be sent to the proper location.



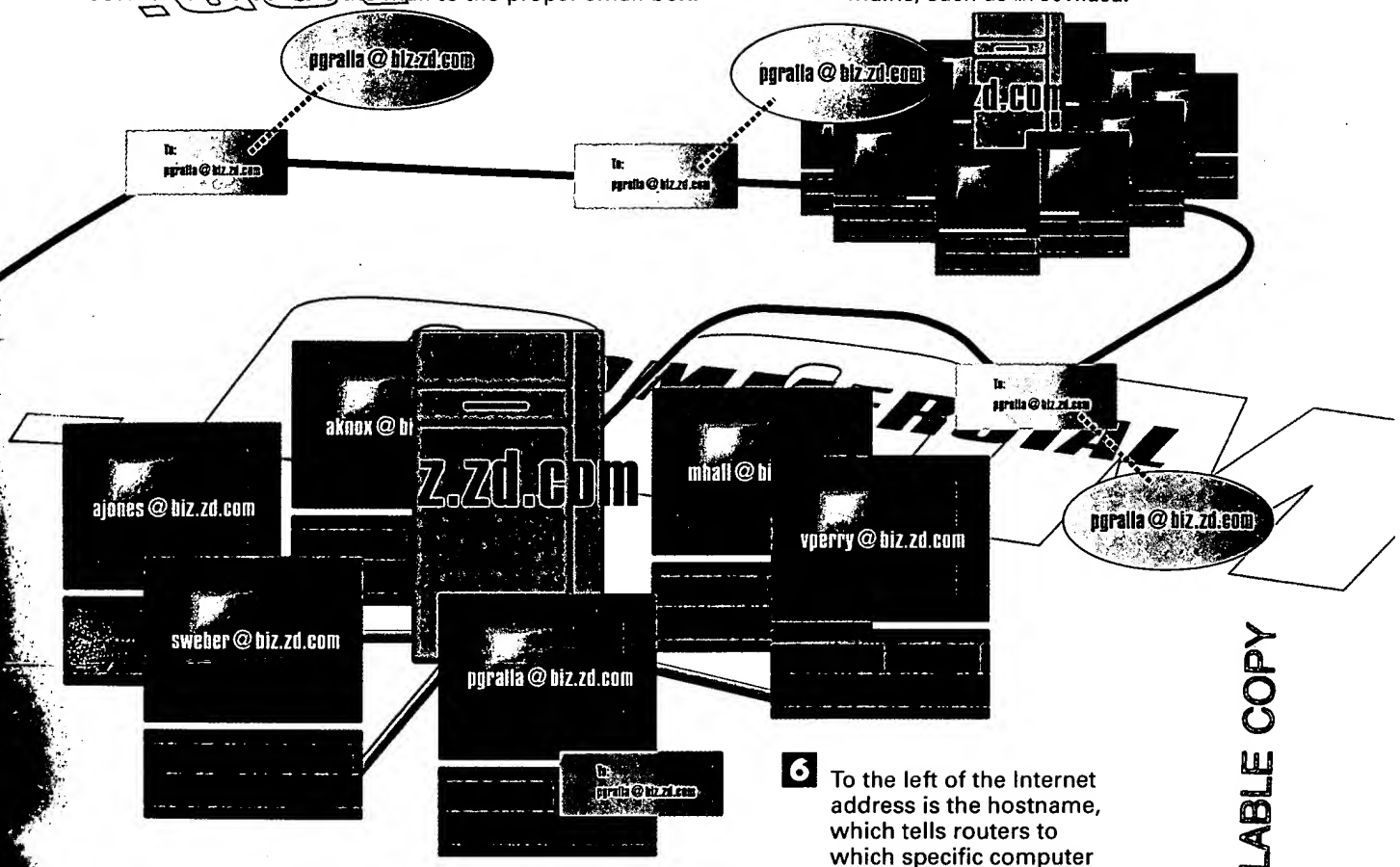
2 An Internet address is made up of two major parts separated by an @ (at) sign. The address can tell you a good deal of information about the person who "owns" the address. The first part of the address (to the left of the @ sign) is the username, which usually refers to the person who holds the Internet account and is often that person's login name or in some way identifies him or her. The second part of the address (to the right of the @ sign) contains the hostname (which can refer to a specific server on a network), followed by the Internet address, which together identify the specific computer where the person has an Internet email account.



3 When you send email, it goes to a name server. In order to deliver the email, the Internet needs to know the numeric IP address, such as 163.52.128.72. Name servers look up the alphabetical address and substitute the numeric IP address for it so the email can be delivered properly.

4 The Domain Name System (DNS) divides the Internet into understandable groups, or domains. Note the portion of the domain section at the far right of the address. It identifies the largest domain names and kind of organization where the person's address resides. The domain names and hostnames identify the host computer where the Internet should deliver the email. The receiving host computer looks at the username and delivers the mail to the proper email box.

5 To the left of the largest domain is specific information about the organization, which tells routers to which network the email should be sent. It can be a single Internet address, such as `zd` (for Ziff-Davis), or it can be a group of domains and subdomains, such as `mfsc.nasa`.



6 To the left of the Internet address is the hostname, which tells routers to which specific computer within the domain the email should be delivered.

7 The domain and hostnames tell the Internet to which computer the email should be delivered. The receiving host computer looks at the username and delivers the mail to the proper email box.

ORGANIZATION